TELECOMMUNICATIONS SWITCH

PROTECTION PROFILE

National Institute for Standards and Technology

Prepared for
Donald Marks
NIST

Prepared by

Bellcore
Ranendra Bhattacharyya

SAIC
Jandria S. Alexander
Robert L. Williamson, Jr.

1 November, 1999
Draft 5.0

Foreword

This publication, Telecommunications Switch Protection Profile, is issued by the National Institute of Standards and Technology as part of its program to promulgate security standards for information systems. This protection profile was developed through the efforts of Dr. Ron Bhattacharyya of Bellcore, and Jandria S. Alexander, Edward J. Coyne, and Robert L. Williamson, Jr. of SAIC.

Comments on this document should be directed to:

Dr. Donald G. Marks
NIST/Computer Security Division
100 Bureau Dr., Stop 8930
Gaithersburg, MD. 20899-8930

(301) 975-5342
donald.marks@nist.gov

TABLE OF CONTENTS

1. Introduction

1.1 Identification

- Title: Telecommunications Switch Protection Profile (TSPP)
- Registration: National Institute of Standards and Technology
- Keywords: Telecommunications, Switch, Information Security

1.2 Overview

The purpose of this document is to develop a Protection Profile (PP) using the Common Criteria (CC) for baseline switch security that is believed to be achievable by deploying currently available Information Technology (IT). It is expected that this PP could be used to develop a uniform test procedure suitable for implementation by appropriate third parties to test the level of security of a wide class of switches, whether stand-alone or coupled with some mediation device. The PP and the ensuing test procedure are intended to be internationally recognized, and endorsed by the industry trade associations. This will provide telecommunications customers with an independent evaluation of security features. The acceptance of these results will improve the security of the entire telecommunications network and allow more open competition among the various switch manufacturers.

A telecommunication switch is an important resource used by telecommunications service providers to provide communications service. In order to ensure the availability, reliability, integrity, and correct billability of this service, it is essential that the switch be secured against unauthorized use and modification/destruction of its embedded processes, software and database.

With the rapid advancement of digital technology, telecommunications switches have evolved from hard-wired, mechanical devices to flexible, dynamic, software-configurable devices. In effect, they have become specialized computers. Access to switch software is no longer only provided from local connections. Remote access for maintenance and configuration management is routinely accomplished via remote access. This remote access has made switches vulnerable to intrusion. The implementation of broadband technology requires a proliferation of specialized switches and connection devices. The resulting diversity and complex inter-connectivity has exacerbated switch vulnerability. The emerging standards that are being developed under Telecommunications Management Network (TMN) are introducing Common Management Information Protocol (CMIP) for switch interfaces in place of proprietary protocols thus increasing the pool of potential attackers. The Communications Assistance for Law Enforcement Act (CALEA) is mandating a new dimension to switch security in order to ensure confidentiality of court-ordered switch-based surveillance. Finally, the nondiscriminatory access to switches, as mandated by the Telecommunications Reform Act of 1996, is causing additional security concerns because networks have to allow equal and nondiscriminatory access to competing service providers. As a result of these developments, switch security has become a critical issue. Indeed, the telecommunications network is considered a “critical infrastructure” and protection of the network is considered to be a high priority for the country.

Meanwhile, with the proliferation of network protocols (e.g., TCP, UDP, IP, etc.), distributed architecture is becoming commonplace wherein switches are becoming nodes in an elaborate network that can provide a wide range of connections to the switch. Consequently, security also is becoming a distributed phenomenon, i.e., security features of a switch may no longer be confined within the switch. For example, a mediation device such as a firewall or a security server may protect a *trusted* network from intruders, and the switch, being a node in that trusted network, may be partially protected by that mediation device. Thus the Protection Profile (PP) of a switch needs to be addressed in terms of security-related functional requirements that have to be satisfied within the environment, either by the switch itself or by mediation devices external to the switch.

1.3 Conventions

This document is organized based on Annex B of Part 1 of the Common Criteria (CC).

Application notes represent guidance and explanations of acceptable implementations for requirements. For additional guidance, the CC itself should be consulted.

1.4 Terms

The following terms, used in this profile, are described in this section to aid in the application of the requirements.

- Mediation Device - This is a peripheral device, external to the switch, which supplements the security of the switch by providing features that are not provided in the switch proper. Examples are firewalls, selective gateways, third party authenticators, security servers, etc.
- Target of Evaluation (TOE) – This is the entity the security of which is being addressed in this Protection Profile (PP). In the case of a stand-alone switch, which constitutes the target, the TOE consists of that switch. However, if a switch is protected by a peripheral security server, the target of security is not just the switch but the total system consisting of the switch and the peripheral security server.
- TOE Security Function (TSF) – This is the hardware-software capability of performing security related functions for the protection of the TOE. Depending on the application, this capability does not need to be confined within the switch. For example, in a networked environment, the required security features can be deployed anywhere in the environment as long as they provide the intended security to the TOE. The functional requirements described in this PP are to be levied on the TSF.
- Authorized Administrator - An authorized administrator is a user who performs administrative tasks such as creating, retrieving, updating and deleting security parameters (e.g., passwords, permission levels, etc.) in the TOE database. As such, the administrator has to be a highly privileged user of the TOE. Depending on the organization, the authorized administrator may have titles such as Security Administrator, System Administrator, etc.

- Customer - A customer is a person or organization that is a subscriber to a service offered by a telecommunications service provider.
- Intruder - An intruder is not authorized to establish a session with the TOE, and as such, is not a user even though the intrusion may be successful.
- Operations Support System (OSS) - An *operations support system* (as distinct from an *operating* system) is a centralized computer environment that remotely performs operation service functions such as provisioning, maintenance, testing, billing, etc., all related to the TOE. There are many types of operations support systems depending on the type of operations functions they perform (an operating system of a TOE, on the other hand, is the underlying platform of the TOE software on which the embedded applications of the TOE reside).
- Owner - The *owner* of a process executing on the TOE. Could be a user, customer, or intruder. Owner is a concept whereby an identified "user" executes a process (unit of execution) within a program, and that process creates an object. The "user" identity associated with the creating process is said to "own" the object created. An owner typically has unlimited access to an "owned object by default (e.g. no administrator action is necessary to provide this access).
- Port - A port represents a point of interface with the TOE. Typically, these ports are attached to the TOE console. Two kinds of ports have been invoked in the PP: (i) the operations port and (ii) the signaling port. Operations ports allow access to the TOE to perform operations functions such as provisioning, maintenance, testing, billing, etc. Signaling ports allow communications devices to be attached to the TOE for the purpose of processing voice and data communication.
- Resource - Broadly speaking, there are two types of resources, namely, hardware resources and software resources associated with a switch. In this PP, the primary focus is on software resources embedded in the TOE. Examples are: the operating system, subsystems, software packages, databases, processes, etc. – all belonging to the TOE.
- Resource Access - Resources are accessed by transmitting messages to the TOE to impact the software resources of the TOE. Examples include loading a patch, creating, modifying and deleting data, retrieving status reports, initiating a process, etc.
- Service - Any function provided to a user by the OSS through an interface designed to provide the service. Services are provided remotely through operations ports, which, in turn, may cause internal services to be provided within the switch. The results of remote services are exported to the user. The results of internal services are used by the TO and typically not exported to the requesting user. For instance, an administrator may submit a remote request to add the name of a maintenance programmer to the list of users allowed access to the switch. In response to this request, the TOE will provide the administrator a response. Internal services provided by the switch, in response to this remote request, may be that the identification of the administrator is first checked, then authenticated before the transaction is allowed. The transaction may be audited for future review. The identification of the maintenance programmer may be placed in a database of users, so the programmer can be authenticated before being allowed access to switch resources and activities can be audited. For each remote service (e.g. operations support) that are pro-

vided, there may be many internal services provided by the TOE. All security relevant services are performed by the TSF.

- Subject – Executing entity within a processor. Typically the smallest identifiable unit of execution for which a specific context is created. For many processors a subject is a *process*.
- System Access - The system is accessed by establishing an operations session (i.e., login) with the TOE. In order to maintain security of the TOE, system access must be successfully completed before resource access is permitted.
- Users - The word “user” is not synonymous with the word “customer”. While a customer is a purchaser of telecommunications service, a user is one that is authorized to establish a session at an operations port of the TOE. Typical users of a TOE consist of craftspersons, administrators, or machines that establish operations related sessions with the TOE. As such, a user could be a person or a machine/system. Hence, all operations support systems are users of the TOE. A valid user must have a user-ID by which the TOE recognizes the user. Accordingly, all operations support systems that access the TOE need to be uniquely identified with an identifier that is presented to the TOE.

2. TOE Description

The TSPP defines a set of security requirements for the protection of a Target of Evaluation (TOE). The requirements are to be levied on the TOE Security Functions (TSF). As mentioned in Section 1.4, a TOE is not synonymous with a "switch". This is because a switch may not be a stand-alone device. A switch often constitutes a node within a distributed architecture consisting of elaborate networks connecting many other switches, mediation devices, and operations support systems. A TOE therefore represents a node in a *switching system* rather than an isolated telecommunications switch. In some cases, it may be assumed that all nodes in the system enforce equivalent security requirements. In other cases, all communication, even from within the system, must be treated with suspicion until the security features are validated. A TOE evaluation is a formal process of analysis and testing to ensure that the defined TOE Security Policy (TSP) is enforced over the TOE resources.

Those hardware-software capabilities that must be relied on for the correct enforcement of the TSP are collectively referred to as the TSF. The TSF consists of all hardware, software, and firmware deployed in the environment (not necessarily within the switch) that is either directly or indirectly relied upon for security enforcement. Any part of the TOE, that is not part of the TSF, may fail or error in any way without violating the TSP. The TSPP lists requirements that need to be satisfied by the TSF for the protection of the TOE.

A switch is a special purpose process control computer that performs *near real time* processing of voice and/or data communication. There is a wide range of switch types including End Office Switch, Local Tandem Switch, Inter-Exchange Carrier Tandem, Signal Transfer Point (STP), various data switches such as ATM, Frame Relay, and Switched Megabyte Data Service (SMDS) switch. Their security requirements may be similar, but their capabilities differ widely because their CPU and memory capacities vary over a wide range. For example, a large end office switch installed in a busy metropolis may have traffic lines in excess of one hundred thousand (100,000) and thirty-to-fifty operations support channels. On the other extreme, a small Ethernet switch may have as few as eight traffic ports and one or two operations channels. Clearly, a security feature that is readily available in one kind of switch may be impractical for another due to CPU and memory limitations. Consequently, it cannot always be expected that a switch will be necessarily equipped with *all* the security features that are needed to protect its embedded resources. Nor is it necessary for each switch to be self-sufficient in its security features as long as there are *mediation devices* deployed within the overall security architecture of the switching system to ensure that the security requirements are satisfied by the TSF. Thus, to secure a TOE, one needs to ensure that the security functions described in this PP are satisfied at an appropriate place within the system.

A switch has two kinds of ports: signal ports and operations ports. The signal ports connect to the communication media (e.g., wires, fiber, cables, trunks) to carry the communications traffic. The operations ports allow ingress into the embedded software of the switch. Crafts-persons and administrators access the operations ports to perform functions such as operations, maintenance, administration, and provisioning. Each operations port is associated with a corresponding set of operations functions. Operations functions may include:

- Line Maintenance,

- Trunk Maintenance,
- Line Testing,
- Trunk Testing,
- Provisioning,
- Recent Change Verification,
- Memory Administration,
- Switching Control Center Connectivity.

Operations ports may also be used to provide vendor-specific functions such as:

- Electronic Technical Assistance (software inputs provided by subject matter experts),
- Automatic Line Identification (printing out the lines that violate the satisfactory operation thresholds),
- Automatic Message Accounting (for billing),
- Engineering Administration Data Systems (EADS - to assess new equipment requirements based on traffic patterns and projections),
- Service Evaluation (monitoring calls to ensure service quality), and
- Software Change Administration and Notification (SCANS - overwriting and patching generic programs).

Crafts-persons authorized to perform operations on the switch may belong to different categories depending on the operations functions performed by them and their level of expertise. This function is filled by the use of different *roles*, as specified in the Common Criteria. Different roles need to have different types of access to specific objects as well as access restricted to specific objects. For example, operations personnel may not need access to billing information. In addition, within the operations personnel a less experienced craft-person may require only “read” permission, while a more experienced person may also require “write” permission. It is even possible for a single person to be authorized different roles. For example, a person who is normally a system administrator may also be authorized to act in the role of an operations person on occasion. Supervisors may be authorized to act in any of the roles filled by people they supervise.

In order to protect switch resources and maintain the quality of service, it is necessary to protect the operations ports from unauthorized use.

3. Security Environment

3.1 Threats

Threats relate to the chance of a security breech that may lead to events such as disclosure of confidential information, commission of fraud, or service deterioration due to modification or destruction of physical and/or Information Technology (IT) resources. Thus the threats that a switch may be subjected to have several dimensionalities. Threats might be caused by outsiders (e.g., intruders) or by insiders (e.g., employees of the service provider). Insider threats are not always a reflection of malice on the part of the employee as they may also be the result of inadvertent employee actions. In order to mitigate these threats, one needs to protect the switch by implementing appropriate security measures.

Examples of threats are listed below.

- Physical threat - Physical damage to a switch may be caused by natural causes such as fire, flood, earthquake, or by human action such as sabotage. This PP assumes that switches are installed in a physically secure environment. Hence physical security is not addressed here as an issue except for cases where it may become unrealistic to ensure physical security, such as in the case of several broadband applications. Broadband switches (e.g., ATM) may be installed without adequate physical protection. Consequently, it becomes necessary to resort to special security measures (discussed later in this PP) to counteract this physical threat.
- Fraud - In the context of telecommunications, fraud implies successfully completing a call (voice or data) without paying the legitimate bill for the call. This can be done in many ways if the service provider does not take proper precautions. Examples of fraud include:
  - Blue Box[1] - A blue box is a device (typically, hand-held) that can generate a 2600 cycles/second tone. It also has a dialing pad that can dial a Directory Number by generating signals that a tandem switch can understand. Incidentally, a tone of 2600cycles/second frequency is used to indicate to the far end carrier to disconnect the call and return supervision to the near end. Consequently, an interloper may place a call to some location via a switch that uses in-band signaling, but before the called party answers, the interloper uses the blue box to generate a 2600cycles/sec tone. Upon receiving the tone, the end office switch at the called location is misled to think that the call is completed and returns control to the initiating phone. However, the transition is incomplete since the far end switch has not yet received the “telephone returned to on-hook position” signal from the end office switch. At this point the interloper may make a call anywhere in the world by dialing that number from the blue box pad. The switch understands that number and connects the call. The bill appears only for the original call.

1 This fraud can be committed only in situations where in-band signaling is still in use. Now-a-days in-band signaling has largely been replaced with Common Channel Signaling, which does not permit blue box fraud.

  - Red Box - A red box is an audio noise generator with a broad audio frequency spectrum. Under certain circumstances, it may be used to make free phone calls from a coin operated phone. If the "Operator Position" is not adequately selective about the actual bandwidth corresponding to the sound of depositing coins, it may be possible to use the red box to fool the operator position into interpreting the noise of the red box as the sound of depositing coins.
  - Eavesdropping for confidential information (e.g., credit card number) - This can be done in several ways, from shoulder surfing to using sniffers to perform wire-tapping.
  - Tumbling Wireless Telephone[2] - An interloper may guess a combination of MIN and ESN and program them into a cloned wireless phone. If the service provider allows a call without validating the MIN/ ESN combination, the interloper may be able to successfully complete the call without having to pay for it. Chances are that the bogus MIN/ESN combination may not belong to any customer, in which case, the service provider may record that information, and deny service the next time the interloper tries to place a call. But the interloper may stay one step ahead by incorporating another MIN/ESN combination which will allow one more call before being denied.
  - Illegally assigning free lines - This requires entering the operations database of a switch to perform illegal provisioning (see Intrusion discussed below).
- Denial of Service – Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration or even denial of service or functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service.
- Access Misuse – Misuse may occur from legitimate users (i.e. insiders performing unauthorized operations) or intruders.
  - A legitimate user may perform an incorrect, or unauthorized, operations function (e.g., by mistake or out of malice) and may cause deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.
  - Intrusion - An intruder may masquerade as a legitimate user and access an operations port of the switch. There are a number of extremely serious threats here, some of which could constitute a crisis. For example, the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:
    - disclosing confidential data[3]
    - causing service deterioration by modifying the switch software
    - crashing the switch
    - removing all traces of the intrusion (e.g., modifying the security log) so that it may not be readily detected

2 With the introduction of validation and authentication of the calling party, the threat of Tumbling has been substantially reduced.

3 There have been cases of illegally obtaining charge card numbers of a large number of customers and selling them for a monitory gain.

- Insecure State Transition - At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:
  - After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, even though new passwords are not yet assigned.)
  - The same may happen at the time of a disaster recovery.
  - At the time of installation the switch may be vulnerable until the default security features are have been replaced.
- Espionage - Competing service providers, utilizing the non-discriminatory access requirement, may attempt to obtain or modify customer information to gain them a competitive advantage.
- Insecure Security System - The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for intruders to use on their next visit. For this reason, the security system must be carefully protected.

3.2 Organizational Security Policies

Organizational security policies (denoted as P.xxx) are normally directed at individual users. However, the binding between users and executable programs is sometimes tenuous, so the term "subject" will be used to describe computer programs or processes when necessary to distinguish them from the actual person initiating the process. Security-related organizational policies include the following:

- P.Access - Access rights to specific objects are determined by object attributes assigned to that object, subject identity, subject attributes, and environmental conditions as defined by the security policy. For an object or a service for which a subject is not authorized access, access shall be denied to that subject.
- P.Accountability - Each user in the organization shall be held accountable for TOE-related actions that they perform.
- P.Administration - The authorized systems administrator shall properly activate, implement and maintain the security features associated with the TSF.
- P.Availability - There shall be no denial of authorized service. A TOE access that a user is authorized for shall not be denied to that user. A service for which a customer is authorized shall not be denied to that customer.
- P.CALEA - The organization shall maintain data confidentiality and controls necessary to comply with the Communications Assistance for Law Enforcement Act (CALEA)[4], which requires the Law Enforcement Agency be allowed "switch-based lawful surveillance under court order."

4 The Safe Harbor Document (# 25J-STD-025) issued by the American National Standards Institute (ANSI) has extended the deadline for CALEA compliance to June 30, 2000.

- P.Confidentiality - Confidential information shall not be made available to unauthorized "users"(persons, machines, etc.).
- P.Resiliency - If a security compromise occurs, the TSF shall alert appropriate administrative staff (see P. Traceability), audit compromised activity, isolate the compromised activity to identified affected subjects and objects (including services) and the TOE shall continue to provide services that were not affected by the compromise.
- P.TMN Standards - The tasks related to “Prevention”, “Detection”, “Containment and Recovery”, and “Security Administration” (as defined under TMN standards) shall be recognized and delegated to appropriate personnel. Prevention implies physical security, legal review, risk analysis, and logical controls. Detection is associated with alarms, recorders, usage pattern analysis, revenue pattern analysis, security audit, investigation of security breech, and other forensic data collection and analysis. Containment and recovery, as the name implies, includes intrusion recovery, disaster recovery, legal actions, apprehension, etc. Security administration involves the day to day activities of ensuring that protective features are activated, the security parameters are kept up to date, and the security weaknesses are corrected.
- P.TRA 1996 - The organization shall comply with the Telecommunications Reform Act (TRA) of 1996, which mandates *Network Unbundling*[5] and non-discriminatory access to corresponding TOE resources for competing service providers.
- P.Traceability - The TSF shall provide features (e.g., alarms, audit trails, etc.) to: (i) alert an administrator of a suspected security breech, and (ii) record security events in a log file so that in case a breech is suspected, an audit trail could be established as part of investigation, and (iii) record adequate audit detail to uniquely identify subjects, ports, and security relevant activities.
- P.Training -Authorized users of the system shall be adequately trained, enabling them to (1) effectively implement organizational security policies with respect to their discretionary actions and (2) support the non-discretionary controls implemented to enforce these policies.
- P.Usage – A TOE shall be used only for authorized purposes.

3.3 Security Usage Assumptions

Assumptions (denoted A.xxx) describe the security aspects of the environment in which the TOE will be used. Implementation details for assumptions are outside the scope of the protection profile. This includes information about the physical, personnel, and connectivity aspects of the environment.

5 Unbundling allows a Competitive Local Exchange Carrier (CLEC) to purchase *access* as well as *use* of individual elements of a network, belonging to the Incumbent Local Exchange Carrier (ILEC), with the purpose of offering its (CLEC’s) own local exchange service. Under the mandate of this “nondiscriminatory access to network elements”, the same switch has to be opened up to competing service providers. Hence its becomes necessary to resolve which provider *owns* which resource within the same switch.

3.3.1. Physical Assumptions

It is assumed that the resources of the TOE, except possibly the remote access facilities, will be installed in a physically secure environment which will be "reasonably safe" from typical natural hazards as well as from unauthorized physical access. An example of a "reasonably safe" system implies the following, as a minimum:

- A.Environment. The TOE shall be protected from environmental hazards.
  - A TOE[6] shall be housed in a facility that shall conform to established local building standards, i.e., codes related to precautions against hazards due to fire, flood, earthquake, and inclement weather conditions such as tornado, hurricane, typhoon, etc. This includes, among other construction codes, appropriate installation of various types of alarms and an administrative mechanism to promptly respond to such alarms when activated.
- A.NoBreakIns. The TOE, and all terminals used for local access, shall be adequately protected from intruders obtaining physical access to the switch or related equipment, by means such as:
  - Lighting within and around a facility shall provide adequate visibility for security guards and cameras,
  - Restricting entry into a facility from outside by means of electronic locks or trained guards & ID cards.
  - Alarming all doors for entering the premises during hours that are outside the normal business hours. Alarming all "exit only" doors (especially emergency exits) all the time.
  - Equipping all facility access points, parking lots or other designated areas with 24-hour camera monitoring.
- A.PhysicalAuthorization. Physical access to the TOE shall be controlled and restricted to those needing such access, through such means as:
  - All persons (i.e., employees, contractors, authorized visitors, etc.) in a TOE facility shall be issued appropriate company-designated badges that authorize the holders to specific facilities or areas which they need to access.
  - Within a given TOE facility, areas which are considered critical/sensitive shall have doors protected with electronic locks that allow entry only to authorized personnel, based on need to access. These doors shall be spring-loaded so that they will automatically close after they have been opened.
  - All visitors to a TOE facility shall sign and date a visitor log, shall be issued a visitor badge and, if necessary, be escorted. The log shall, as a minimum, record the visitor's name, the name of the establishment he/she represents, citizenship, the TOE point of contact, purpose of visit, date and times of arrival and departure.
  - All visitor badges shall be date and time limited.
- A.TRA. If several competitors have their presence in the same physical facility (such as may be required for TRA compliance), there shall be sub-areas and physical barriers, to the extent feasible, to keep their respective physical resources separate from one another.

6 Exceptions are the ubiquitous switches, such as broadband switches and routers, for which it may not always be feasible to guarantee a physically secure environment.

3.3.2. Personnel Assumptions

It is assumed that the following personnel conditions will exist:

- A.Audit. Internal auditors as well as external auditors shall be available to conduct periodic security audits (reviews);
- A.Clearance. Each TOE owner will have a formal process to be completed before a person may be deemed "responsible". This process may include interviews, checking references, or an extensive background check;
- A.Expertise. Responsible individuals shall be available to perform the tasks associated with Prevention, Detection, Containment & Recovery, and Security Administration, as described in Section 3.2;
  - Security analysts shall be available to perform security analysis (i.e., testing the security features for conformance and nonconformance with PP) for new hardware and software before they are installed.
- A.Redress. Each TOE owner will have redress available to hold users accountable for their actions. Such redress may be either legal or administrative actions; and
- A.Training. Individuals shall receive an appropriate level of security training.
  - There shall be at least a minimum level of security awareness among all personnel.
  - Individuals deemed critical for secure operation shall receive additional training in security awareness and operational issues.

3.3.3. Connectivity Assumptions

Telecommunications switches are routinely connected to a network containing many other devices. The overriding security principle in such a networked environment is that there can be no assumptions made about the security features of these other devices or the network itself. That is, everything is assumed to be insecure unless known otherwise. Specifically, it is assumed that the following connectivity assumptions exist:

- A.Ingress. It is assumed that there are three types of ingress into the operations ports of a switch, namely, local access, remote dial-up access, and remote networked access;
  - Operations Support Systems (OSS), in general, shall access the switch from remote locations, either via dial-up access or via networked access.
    There may be human users who are authorized to access the switch from terminals situated at remote locations, and they may use dial-up access or networked access directly to the switch.
- A.InsecureNetwork. The network is assumed to be insecure except for known security capabilities;
- A.InsecureRemote. Remote locations shall be assumed to be insecure, except for security capabilities known to be installed at that particular location; and
- A.Protocols. Networked accesses may use a wide range of protocols such as X.25, TCP/IP, CMIP, SNMP, SS7 (for Common Channel Signaling), and several proprietary protocols.
- A.Hardware. The switch hardware shall support the required functions.

4. Security Objectives

This section defines the security objectives of the TOE (denoted O.xxx) and its supporting environment. Security objectives, categorized as either Technical security objectives or non-Technical security objectives, reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. All of the identified threats and organizational policies that are addressed by this PP can be found under one or more of the categories below.

4.1 Technical Security Objectives

- **O.DOMAIN SEPARATION:** The TSF shall create and maintain a separate domain or domains of execution in which it can execute without interference from all subjects outside of this domain.
- **O.KNOWN**: The TSF shall ensure that, except for a well-defined set of allowed actions, all users are identified and authenticated before being granted access to the TOE or its resources.
- **O.ACCESS**: The TSF shall allow access by authenticated users to those TOE resources for which they have been authorized, and deny access to those TOE resources for which they are not authorized.
- **O.AUTHORIZE**: The TSF shall provide the ability to specify and manage “resource access permission” to be assigned to its users.
- **O.BYPASS**: The TSF shall prevent all software and users from bypassing or circumventing TOE security policy enforcement.
- **O.MISUSE**: The TSF shall mitigate the threat of malicious actions by authenticated users (e.g. by holding all authenticated users accountable).
- **O.ACCOUNT**: The TSF shall ensure that all TOE users can be held accountable for their security-relevant actions.
- **O.INFO-FLOW**: The TSF shall ensure that any information flow control policies are enforced - (1) between TOE components and (2) at the TOE external interfaces.
- **O.OBSERVE**: The TSF shall ensure that its security status is not misrepresented to the administrator or user.
- **O.DETECT**: The TSF shall have the capability to detect system failure and breech of security.
- **O.RECOVER**: The TSF shall provide for recovery to a secure state following a system failure, discontinuity of service, or detection of a security flaw or breech.
- **O.AVAILABLE**: The TSF shall protect the TOE from denial-of-service attacks, including those due to shared resource exhaustion.
- **O.NETWORK**: The TSF shall have the capability to meet the TOE security objectives in a networked environment.
- **O.CONFIDENTIAL**: The TSF shall have the ability to identify confidential information. Such information may be related to customers, system security, TRA or CALEA. The TSF shall release confidential information only to authorized users.

4.2 Non-Technical Security Objectives

- **O.COMPLY**: The TOE environment must support full compliance with laws, regulations, and contractual agreements;
- **O.MANAGE**: An administrator responsible for TOE security shall ensure that the TOE is managed and administered in a manner that maintains security;
- **O.OPERATE**: An administrator responsible for TOE security shall ensure that the TOE is delivered, installed, and operated in a manner which maintains security; and
- **O.PHYSICAL**: An administrator responsible for TOE security shall ensure that the TOE environment has adequate physical security to provide "reasonable safety" (as described earlier) to TOE resources.

4.3 General Assurance

It is desirable that applications, which require numerous switch installations, (such as ATM switches in the case of broadband applications), shall provide layered security administration, in compliance with TMN standards. These standards specify five layers defined as:

1. Business Management Layer (BML) - which will be responsible for tasks such as Security policy, Disaster recovery plan, Assessment of data integrity, etc.
2. Service Management Layer (SML) - which will perform functions such as Administration of certification, Administration of security protocols, Customer audit trail management, and Customer security alarm management.
3. Network Management Layer (NML) - which will perform administration of security parameters at the overall network level.
4. Element Management Layer (EML) - which will perform administration of security parameters of a group of similar switches.
5. Network Element Layer (NEL) - which will provide local access at the switch console.

It follows from the above definitions, that while BML and SML take care of the business and service related concerns associated with security, the three lower layers, namely, NML, EML, and NEL perform the switch operations in a hierarchical way. Hence it is assumed that, as a minimum, these three layers will provide the required connectivity for broadband switch operations.

As discussed earlier, the TOE needs to have CALEA compliance, which requires that law enforcement agencies be provided with switch-based lawful surveillance under a court order. This means that when law enforcement approaches a service provider, it is for the service provider to obey the court order and provide the law enforcement agency with the relevant surveillance data collected from the switch. Consequently, there must be a port of the switch dedicated to CALEA related activity. Due to the confidential nature of surveillance activity, this special port of the switch and its connectivity must be kept off limits for all users that are not authorized access to these activities. It is also important to ensure that an intruder does not access this port and perform unauthorized surveillance.

The TOE also has to comply with the Telecommunications Reform Act (TRA) of 1996, which mandates that competing service providers must be allowed nondiscriminatory access to certain network components (*Network Unbundling*). The resources for each service provider shall be kept confidential from other service providers.

TOEs compliant with this PP are targeted for near-term achievable, cost-effective, Commercial Off-The-Shelf (COTS) security. In keeping with this target, the general level of assurance for TOEs must:

- Be consistent with current best commercial practice for Telecommunications development; and
- Enable evaluated products that are competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

TOEs compliant with this PP must meet an appropriate formal assurance level in order to be consistent with current and near-term mutual recognition agreements. This requires that the assurances:

- Be expressed as an existing evaluation assurance level (EAL) from part 3 of the Common Criteria; augmented by CC assurance components as required; and
- Contain no assurance components first appearing in EAL5 or above

Although most computer security products only meet level EAL2, the telecommunications industry is, in general, concerned with reliability, security, and good software engineering techniques. This care in the software development and design provides a higher assurance level for telecommunications switches than for most commercial computer software products. Therefore, EAL3 was selected as a reasonable target for this PP.

5. Functional Requirements

The policies, assumptions, and objectives generally define high-level descriptions of desirable security features. These high-level statements are implemented by combinations of low-level, specific functions. This chapter defines these functional requirements for the TSF. Functional requirement components in this profile were drawn from Part 2 of the CC.

CC defined operations for assignment, selection, and refinement are used to tailor the requirements to the level of detail necessary to meet the stated security objectives (Section 4.1). The use of these operations does not constrain TOE implementation, and all required operations not performed within this profile are clearly identified and described such that they can be correctly performed upon instantiation of the PP into a Security Target (ST) specification.

5.1 Protection of the TOE Security Functions (FPT)

5.1.1. Abstract Machine Testing (FPT_AMT.1)

The TOE Security Functions will depend upon the proper functioning of the underlying hardware and primitive operating system functions such as device drivers, protocol handlers, or hardware page protection. This underlying hardware/software platform will vary by manufacturer, but the *abstract* functions will be identical. The combination is therefore referred to as an *abstract machine*, and must be periodically tested for correct operation although its functions are not covered by the Protection Profile.

5.1.1.1 FPT_AMT.1.1. The TSF shall run a suite of tests at the request of an authorized administrator to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.1.2. Fail Secure (FPT_FLS.1)

5.1.2.1 FPT_FLS.1.1. The TSF shall preserve a secure state when the following types of failures occur:

- Audit log overflow.
- Failure of individual channels or ports.
- Failure of trunk.
- Failure of lines.

5.1.3. Inter-TSF trusted channel (FPT_ITC.1)

5.1.3.1 FTP_ITC.1.1. The TSF shall protect sensitive TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

5.1.4. Inter-TSF detection and correction of modification (FPT_ITI.2)

5.1.4.1 FPT_ITI.2.1. The TSF shall provide the capability to detect modification of sensitive TSF data during transmission between the TSF and a remote trusted IT product within appropriate limits as selected by the TOE owner.

5.1.4.2 FPT_ITI.2.2. The TSF shall provide the capability to verify the integrity of sensitive TSF data transmitted to the TSF from a remote trusted IT product and perform the necessary specified actions if modifications are detected.

5.1.5. Automated Recovery (FPT_RCV.2)

5.1.5.1 FPT_RCV.2.2. For a selected list of failures, the TSF shall ensure the return of the TOE to a secure state using automated procedures.

5.1.5.2 FPT_RCV.2.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a secure state where the ability to manually return the TOE to a secure state is provided.

5.1.6. Reference Mediation (FPT_RVM.1)

The requirements of this family address the “always invoked” aspect of a traditional reference monitor. The goal of this family is to ensure, with respect to a given TSP, that all actions requiring policy enforcement are validated by the TSF.

5.1.6.1 FPT_RVM.1.1. The TSF shall ensure that the TSP enforcement functions are invoked and succeed before any security relevant function within the TOE is allowed to proceed.

5.1.7. Domain Separation (FPT_SEP.1)

The components of this family ensure that at least one security domain is available for the TSF’s own execution and that the TSF is protected from external interference and tampering (e.g. by modification of the TSF code or data structures) by untrusted subjects.

5.1.7.1 FPT_SEP.1.1. The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

5.1.7.2 FPT_SEP.1.2. The TSF shall enforce separation between the security domains of subjects in the TOE.

5.1.8. Simple trusted acknowledgement (FPT_SSP.1)

5.1.8.1 FPT_SSP.1.1. The TSF shall acknowledge, when requested by another part of the TSF, the receipt of unmodified TSF data transmission.

5.1.9. Reliable Time Stamps (FPT_STM.1)

5.1.9.1 FPT_STM.1.1. The TSF shall be able to provide reliable time stamps for its own use.

5.2 Identification and Authentication (FIA)

5.2.1. Authentication Failure Handling (FIA_AFL.1)

5.2.1.1 FIA_AFL.1.1. The TSF shall detect when an administrator-selected number of unsuccessful authentication attempts occur related to consecutive login failures.

5.2.1.2 FIA_AFL.1.2. When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall

- block new attempts for the amount of time set by the authorized administrator, and
- send a notification to the authorized administrator.

5.2.2. User Attribute Definition (FIA_ATD.1)

5.2.2.1 FIA_ATD.1.1. The TSF shall maintain the following list of security attributes belonging to each individual user:

- User Identifier;
- Roles;
- Authentication Data, such as passwords;
- Port and Channel permissions;
- Other user security attributes as may be specified by an authorized administrator.

5.2.2.2 FIA_ATD.1.2. The TSF shall maintain the following security attributes only in encrypted form

- User passwords;
- Other selected user attributes as designated by the security administrator.

5.2.3. Strength of Authentication Data (FIA_SOS.1)

5.2.3.1 FIA_SOS.1.1. The TSF shall provide a mechanism to verify that confidential parameters that are used for authentication meet a quality metric defined by the authorized administrator.

For example: passwords may be required to be a minimum of 8 characters long and contain at least one number.

5.2.4. Timing of Authentication (FIA_UAU.2)

5.2.4.1 FIA_UAU.2.1. The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on be behalf of that user.

5.2.5. Multiple-use authentication mechanisms (FIA_UAU.5)

5.2.5.1 FIA_UAU.5.1. Depending on the application, the TSF shall provide one or more of the following authentication mechanisms to support user authentication: passwords, dial-back modems, one-time authentication devices, etc.

5.2.5.2 FIA_UAU.5.2. The TSF shall authenticate any user's claimed identity according to the [assignment:

For remote logins over untrusted paths (i.e., switched or networked links that do not validate the user) the TSF shall employ a supplemental authentication mechanism. At least one of the following mechanisms shall be employed:

- Secure dial-back using smart modems providing the following functions:
  - The modem, after receiving a login request from a remote location, shall disconnect the line before dialing the *authorized number* to re-establish the contact.
  - The dial-back shall be performed over a line different from the line over which the login request arrived at the modem.
  - A loss of power to the modem shall not cause the modem to revert back to a default state of any sort.
  - The password file in the modem shall be readable only by a the security administrators.
  - The modem configuration shall be modifiable only by the security administrators who are authorized to do so.
- Selective call acceptance based on the validity of the calling address for remote login request made over a three-layer protocol (i.e., do not allow the login unless the remote address is authorized for login).
- Token type authenticator where a remote user is validated by verifying the correctness of a random number generated by the user's token.
- Trusted centralized authentication server (such as Kerberos™[7]) to authenticate a third party user.
- Public-key/private-key encryption technology to authenticate remote users.
- The TSF shall not allow unauthenticated access from a remote source (e.g., .rhost) unless the source is adequately protected against intrusion and the link between the two is encrypted.
- If unauthenticated access is provided via a protocol such as Simple Network Management Packet (SNMP) – Version 1, the TSF shall have the capability to disable such direct accesses.]

5.2.6. Protected authentication feedback (FIA_UAU.7)

5.2.6.1 FIA_UAU.7.1 The TSF shall provide only minimal feedback to the user while the authentication is in progress.

- The TSF shall not transmit a response to any part of the login sequence until the entire login sequence has been completed.

7 Kerberos is a trademark of MIT.

- Upon successful login, the TSF shall display the date and time of the last successful login by the user and the number of unsuccessful attempts (if any) since the last login, and shall optionally require an acknowledgement thereof.

5.2.7. User Identification Before Any Action

5.2.7.1 FIA_UID.2.1 The TSF shall require each user, process or application to identify itself before allowing any other TSF-mediated actions on behalf of that user, process or application.

5.2.8. User-Subject Binding (FIA_USB.1)

5.2.8.1 FIA_USB.1.1. The TSF shall associate the appropriate user security attributes with subjects acting on the behalf of that user:

- The user identity which is associated with auditable events;
- The user identity or identities which are used to enforce Roles.

5.3 TOE Access (FTA)

5.3.1. Limitation on scope of selectable attributes (FTA_LSA.1)

5.3.1.1 FTA_LSA.1.1. The TSF shall restrict the scope of the session security attributes [assignment: access permissions, audit requirements, other session security attributes] based on [assignment: session type, ports, network identification of the specific requestor, date and time, other attributes].

For example, if an *output port* receives a login request, the port shall not respond. The TSF shall have the capability to restrict a login based upon the time, date, and network identification of the specific requestor/process.

5.3.2. TSF-initiated session locking (FTA_SSL.1)

5.3.2.1 FTA_SSL.1.1. The TSF shall lock an interactive session after [assignment: *time interval of user inactivity*] by:

- Clearing or overwriting display devices, making the current contents unreadable;
- Disabling any communication with the user's data access/display devices other than re-establishing the session.
- For ports dedicated to interactive sessions, the TSF shall lock the port for subsequent *inputs*, other than re-authentication actions, although the TSF shall be able to transmit over the locked port.

5.3.2.2 FTA_SSL.1.2. The TSF shall require the following events to occur prior to unlocking the session:

- Identification/authentication of the user either to the switch or to another trusted network device
- [assignment: Other events as specified by an authorized administrator].

Application Note: Sessions established by other network components that are identified and authenticated as "users" are not considered interactive sessions. The TSF shall have the capability of distinguishing between these two types of sessions, for example through differing login procedures. The TSF may then disable the time-out feature for network component sessions even if they stay logged on to the TOE for extended periods of time.

5.3.3. User-initiated session locking (FTA_SSL.2)

5.3.3.1 FTA_SSL.2.1. The TSF shall allow user-initiated locking of the user’s own interactive session, by:

a. clearing or overwriting display devices, making the current contents unreadable;
b. disabling any activity of the user’s keyboard or other data access/display devices other than unlocking the session.

5.3.3.2 FTA_SSL.2.2. The TSF shall require the following events to occur prior to unlocking the session:

a. re-authentication of the user
b. [assignment: Other events as specified by an authorized administrator].

5.3.4. TSF-initiated termination (FTA_SSL.3)

5.3.5. TSF-initiated termination (FTA_SSL.3)

5.3.5.1 FTA_SSL.3.1. The TSF shall terminate an interactive session after a [assignment: time interval of user inactivity, power failure, link disconnection].

5.3.6. Default TOE access banners(FTA_TAB.1)

5.3.6.1 FTA_TAB.1.1. At the time of login, the TSF shall generate a warning banner.

The message transmitted in the banner shall be specifiable by an authorized administrator to meet local requirements and state and federal laws.

5.3.7. TOE access history (FTA_TAH.1)

5.3.7.1 FTA_TAH.1.1. Upon successful login, the TSF shall display the [selection: *date, time, method, location*] of the last successful login, the number of unsuccessful attempts (if any) since the last login, and the date and time of the last unsuccessful attempt.

5.3.7.2 FTA_TAH.1.2. Upon successful session establishment, the TSF shall display the [selection: *date, time, method, location*] of the last unsuccessful attempt to establish a session and the number of unsuccessful attempts since the last successful session establishment.

5.3.7.3 FTA_TAH.1.3. The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

5.3.8. TOE Session establishment (FTA_TSE.1)

5.3.8.1 FTA_TSE.1.1. The TSF shall be able to deny session establishment based on [assignment:

- When a session is terminated (i.e., when a logoff occurs), the port shall drop immediately so that a subsequent user has to re-authenticate to initiate the next session.
- Before allowing a session (i.e., a login), the TSF shall require a session requester to provide the identifier as well as the authenticator. All access ports, except the Emergency

Access Interface[8] (EAI) or a port with similar functions, shall be equipped with this login feature.

- The EAI shall have the following features to provide protection against intrusion: The TSF shall activate a verifiable alarm that requires acknowledgement when the EAI is in operation. The TSF shall prevent the EAI from accepting any commands other than those considered essential for performing system restoration.
- If unauthenticated access is provided over a Data Communications Channel (DCC), as in the case of a Synchronous Optical Network (SONET), the TSF shall control access, if necessary by using a peripheral device such as a firewall.
- The TSF shall provide a dedicated port of access to provide court-ordered *switch-based* surveillance in conformance with the Communications Assistance for Law Enforcement Act (CALEA). The TSF shall ensure that the *usage* of this port as well as *messages* occurring at this port remain confidential from all other users logged on to other ports of the TOE, including the administration port.
- If the TOE architecture consists of numerous distributed elements such that the management of identification and authentication information for all network elements on an individual basis becomes unrealistic, the architecture shall deploy a centralized mediation device such as an Element Management System (EMS) which shall have the capability to deny local login requests to any specific network element (e. g., disable the *local points of ingress*[9] into all the network elements) by executing an appropriate command which all the network elements under the control of the EMS shall recognize, act upon and acknowledge].

Application Notes:

- All software changes shall be documented and reviewed to ascertain that security has not been compromised.
- The TOE shall be delivered with secure installation defaults.
- An administrator shall have the capability to customize the default security parameters (e.g., default user identifiers, default authenticators, default settings for access permission levels for various system resources, etc.) at any time during the installation process.
- The TOE shall generate warning messages if changes could have the affect of reducing security.
- There shall be test procedures to determine whether the delivered software is exactly as specified in the master copy.

---

8 A switch may be equipped with an EAI which allows a session without requiring a login so that in the case of an emergency, when the regular login feature does not function, the switch, as a minimum, can be restored via the EAI. There are ways to protect the EAI against intrusion, as described in the next requirement.

9 A local point of ingress means an entry port at the switch console. If intrusion at the switch console is suspected, all such entries need to be locked out by a command from a centrally located EMS. This is because numerous broad band switches may be distributed over a wide area, where it may not be feasible to physically protect against all local accesses. Nor may it be feasible to perform password management for a large number of users. Consequently, such switches should be required to recognize the “lock out command” from the EMS and respond accordingly.

5.4 Cryptographic Support (FCS)

5.4.1. Cryptographic Operation (FCS_COP.1)

All cryptographic operations shall comply with applicable national, international, and local laws, rules, regulations and treaties.

5.4.1.1 FCS_COP.1.1.

The TSF shall support the Telecommunications Management Network (TMN) based switch management system specified by the International Telecommunication Union (ITU) to provide protection for transactions between switches and the integrity of the Common Management Information Protocol (CMIP) based messages that are exchanged between a switch and an OSS. To provide this functionality, the TSF shall either support the "Security Transformations Application Service Element for Remote Operations Service Element" (STASE-ROSE) as described in Section 5.4.1.2 or the alternative specified in Section 5.4.1.3.

The TSF shall support the default public key authenticator defined in the standard T1.259, along with exchange of a symmetric session key.

5.4.1.2 STASE-ROSE

STASE-ROSE shall support the following security transformations (STs)[10]:

- **Confidential:** The DER-encoded ROSE PDU shall be encrypted for privacy protection with a symmetric key encryption algorithm.
- **Hashed:** a hash-based Message Authentication Code (MAC) of the DER-encoded ROSE PDU and a secret password shall be calculated and the results appended to the ROSE PDU for integrity protection.
- **Confidential hashed:** The MAC of the DER-encoded ROSE PDU shall be computed and the results appended to the encrypted (see "confidential" above) ROSE PDU for integrity and privacy protection.

5.4.1.3 STASE-ROSE Alternative for TCP/IP

If all network management transactions are transported over TCP/IP, it is not required for the TSF to support STASE-ROSE. If STASE-ROSE is not provided by the TSF for TCP/IP transactions, the TSF shall use the Secure Socket Layer version 3 (SSL3) or IPSec. The TSF implementation of SSL3 shall support the following:

- strong peer entity authentication, based on public key encryption shall be provided for all associations (this precludes interoperability with SSL2)
- session secrets shall be encrypted with intended receiver's public key
- Secure Hash Algorithm 1 (SHA1) shall be used for integrity by SSL3

10 STASE-ROSE protects ROSE PDUs by applying selected security transformations (ST) to whole ROSE PDUs encoded with the Distinguished Encoding Rules (DER).

- if privacy protection by SSL3 is provided, then DES-3 (Triple Data Encryption Standard) in the CBC (Cipher Block Chaining) mode shall be used for symmetric key encryption
- integrity and non-repudiation shall be computed on clear text (unencrypted) messages,
- a public key certificate from the TMN's Certificate Authority (CA) message is required
  - Certificates shall be X.509 version 3
  - the CA's public key size shall be at least 1024 bits
  - entity public key size shall be at least 768 bits
- The following cipher-suites will be supported:
- RSA, NULL, SHA1 (if no privacy protection is desired)
- RSA, DES3 - CBC, SHA1 (if privacy protection is desired)

The TSF implementation of IPsec shall support the following:

- strong peer entity authentication, based on public key encryption shall be provided for all associations
- session secrets shall be encrypted with intended receiver's public key or negotiated through IKE
- Integrity shall be provided using the ESP header with HMAC-SHA1
- if privacy protection is provided, then DES-3 (Triple Data Encryption Standard) in the CBC (Cipher Block Chaining) mode shall be used for symmetric key encryption
- a public key certificate from the TMN's Certificate Authority (CA) message is required
  - Certificates shall be X.509 version 3
  - the CA's public key size shall be at least 1024 bits
  - entity public key size shall be at least 768 bits
- The following cipher-suites will be supported:
- NULL, HMAC-SHA1 (if no privacy protection is desired)
- DES3 - CBC, HMAC-SHA1 (if privacy protection is desired)

5.5 User Data Protection (FDP)

5.5.1. Complete Access Control (FDP_ACC.2)

5.5.1.1 FDP_ACC.2.1 The TSF shall enforce the TOE Access Control Policy on all subjects and objects and all operations among subjects and objects covered by the TSP.

5.5.1.2 FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TOE and any object within the TOE are controlled by an access control mechanism as described in the TSP.

5.5.2. Access Control Functions (FDP_ACF.1)

5.5.2.1 FDP_ACF.1.1. The TSF shall enforce the Access Control Policy on subjects and objects based on [assignment:

- The user identity and group membership(s) associated with a subject (e.g., a privilege associated with the user ID)
- The access control attributes and permissions associated with an object
- Rule(s) defined by authorized administrators that allow or deny operations based on (a) and (b).
- Rule(s) defined by an authorized administrator that allow or deny access on the basis of parameters other than those described in (a) and (b), e.g., rules based on time of the day, port, or location.]

5.5.2.2 FDP_ACF.1.3. The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: administrator-defined rules that explicitly authorize access of subjects to objects based on security attributes].

5.5.2.3 FDP_ACF.1.4. The TSF shall explicitly deny access of subjects to objects based on the following rules: [assignment:

- The TSF shall not allow *resource access* to any user who has not established *system access* (i.e., a login with identification and authentication).
- The TSF shall deny the access to a resource unless a user has permission to access that resource.
- The TSF shall deny the access to a resource to all users logged into a port unless that port has permission to access that resource.
- The level of granularity of the resource control mechanism shall be such that, any given user that has logged into any given port can be granted access or denied access to any given resource (based on the user privilege and the port privilege).
- The TSF shall have the capability to prevent execution of potentially damaging commands (e.g., delete all translations) based upon user privilege and port privilege.
- If the TOE serves as a Signaling Transfer Point (STP) with a *built-in device* for testing the Common Channel Signaling (CCS) network by transmitting Signaling System-7

(SS7) signals, the TSF shall have the capability to restrict access to the built-in testing device only to authorized users[11].

- The TSF shall have the capability to impose access control on the basis of functions such as Create, Read, Update, and Delete (CRUD).
- The TSF shall not permit any mechanism to bypass authorization restrictions.
- The TSF shall not permit a less privileged user to spoof as a highly privileged user (such as a Superuser in a UNIX environment).
- Pursuant to the Telecommunications Reform Act (TRA) of 1996, which mandates *Network Unbundling*[12] the TSF shall protect the confidentiality of one party's resources from other collocated parties.
- The TSF shall require that user privileges (i.e., access permissions) be assigned to user-IDs (not passwords[13]).
- the TSF shall not allow voice or data transmission from the TOE to a Customer Premises Equipment (CPE) until the CPE specifically communicates to the TSF that the "off hook" status has been initiated in the CPE.[14]
- The TSF shall require that resource privileges be assigned to input ports.]

5.5.3. Residual Information Protection (FDP_RIP.2)

5.5.3.1 FIP_RIP.2.1. The TSF shall ensure that any previous information content of a resource is made unavailable upon the re-allocation of the resource to any object - except for references contained in the audit trail.

11 An unauthorized user accessing a testing device could transmit bogus SS7 messages to cause severe service deterioration, e.g., crashing the CCS network.

12 Unbundling allows a Competitive Local Exchange Carrier (CLEC) to purchase *access* as well as *use* of individual elements of a network, belonging to the Incumbent Local Exchange Carrier (ILEC), with the purpose of offering its (CLEC's) own local exchange service. Under the mandate of this "nondiscriminatory access to network elements", the same switch has to be opened up to competing service providers. Hence its becomes necessary to resolve which provider *owns* which resource within the same switch.

13 Assigning user privileges to passwords may compromise their confidentiality.

15 This is a precautionary measure to reduce the threat of Black Box fraud.

5.6 Security Audit (FAU)

5.6.1. Security Alarms (FAU_ARP.1)

- FAU_ARP.1.1. The TSF shall take [assignment: *list of the least disruptive actions*] upon detection of a potential security violation.

5.6.2. Audit Data Generation (FAU_GEN.1)

5.6.2.1 FAU_GEN.1.1. The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the basic level of audit, including:
  - Modifications of security attributes;
  - Attempts to revoke security-relevant authorizations;
  - Attempts to revoke access rights;
  - Changes to the time;
- [assignment: Other specifically defined auditable events:
  - Changes to system software that is part of the TOE that lies outside the TSF. Modification to the TSF is not allowed, once evaluated; however modification to other essential software (e.g. billing) that does not affect the security policy may be modified.]

5.6.2.2 FAU_GEN 1.2. The TSF shall record within each audit record at least the following information:

- System date and time of the event, type of event, subject identity, and the outcome (success or failure[15]) of the event.
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST [assignment:
  - For Identification and Authentication events, the origin (e.g., terminal identification) of the attempt.
  - For modifications to TSF data, the old and new values of the data.
  - For the use of the rights of a role[16], when it could originate from multiple locations, the origin of the attempt.
  - *Other audit relevant information identified in the ST*:]

15 Application Note: Failures need not record a discrete event in the audit log. Failures may be recorded as the collection of several positive events.

16 Application Note: For example, administrators may logon to a console or an alternate location.

5.6.3. User Identity Association (FAU_GEN.2)

5.6.3.1 FAU_GEN.2.1. The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Application Note: the audit requirements therefore must include:

- For each event recorded in the security log, the TSF shall also record the identifier of the user (the user-ID) that is accountable for the event.
- For software and data created or modified in the TOE, the TSF shall provide administrators the capability to retrieve the user-ID, date and time associated with that creation or modification.

5.6.4. Potential violation analysis (FAU_SAA.1)

5.6.4.1 FAU_SAA.1.1. The TSF shall apply a set of rules in monitoring the audited events and base these rules upon potential violations of the TSP.

5.6.4.2 FAU_SAA.1.2. The TSF shall enforce the following rules for monitoring audited events:

- Accumulation or combination of [assignment:
  - *logon failures known to indicate a potential security violation;*
  - *other rules as identified in the Security Target*].
- [assignment: *any other rules*].

5.6.5. Audit Review (FAU_SAR.1)

5.6.5.1 **FAU_SAR.1.1**. The TSF shall provide authorized administrators with the capability to read [assignment:

- *Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.*
- *For applicable events, the names of the resources accessed.*
- *For Identification and Authentication events, the origin (e.g., terminal identification) of the attempt.*
- *For modifications to TOE data, the old and new values of the data.*
- *For the use of the rights of a role, when it could originate from multiple locations, the origin of the attempt.*
- *Other audit relevant information.*]

from the audit records.

5.6.5.2 **FAU_SAR.1.2**. The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.6.6. Restricted Audit Review (FAU_SAR.2)

5.6.6.1 **FAU_SAR.2.1.** The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.6.7. Guarantees of Audit Data Availability (FAU_STG.2)

5.6.7.1 **FAU_STG.2.1**. The TSF shall protect the stored audit records from unauthorized deletion, change, replacement, insertion, verification or disclosure.

5.6.7.2 **FAU_STG.2.2.** The TSF shall be able to detect modifications to the audit records.

5.6.7.3 **FAU_STG.2.3.** The TSF shall ensure that the capacity of the audit file is sufficient to store at least 24 hours of audit records even when the following conditions occur: audit storage exhaustion.

5.6.8. Action in case of possible audit data loss (FAU_STG.3)

5.6.8.1 **FAU_STG.3.1.** The TSF shall send an alarm requiring an acknowledgement to the authorized administrator if the audit trail exceeds an authorized administrator defined limit.

5.6.9. Prevention of Audit Data Loss (FAU_STG.4)

5.6.9.1 **FAU_STG.4.1.** The TSF shall overwrite the oldest stored audit records if the audit trail is full.

5.7 Security Management (FMT)

5.7.1. Management of Security Functions (FMT_MOF.1)

5.7.1.1 FMT_MOF.1.1. The TSF shall restrict the ability to:

- *determine the behavior of,*
- *enable,*
- *disable, and*
- *modify the behavior of*

the functions [assignment:

- *Audit,*
- *Password Management,*
- *Roles,*
- *Users management, and*
- *other functions*]

to [assignment: *authorized administrators, other authorized identified roles*]

5.7.2. Management of Object Security Attributes (FMT_MSA.1)

5.7.2.1 FMT_MSA.1.1. The TSF shall enforce the *Access Control Policy* to restrict the ability to *modify* the security attributes: [assignment: *userid, password, roles, or other security attributes associated with a named object*] to *the authorized identified roles.*

5.7.3. Management of the Security Data (FMT_MTD.1)

5.7.3.1 FMT_MTD.1.1. The TSF shall restrict the ability to *create, delete, and clear* the [assignment: *audit history file, other TSF data*] to [assignment: *system administrators, other authorized security roles*].

6. Assurance Requirements

This chapter defines the assurance requirements for the TOE from Part 3 of the CC.

Assurance is grounds for confidence that an IT product or system meets its security objectives. The CC provides assurance through active investigation. Active investigation is an evaluation of the IT product or system in order to determine its security properties.

Each assurance element is identified as belonging to one of the three sets of assurance elements:

a. Developer action elements: the activities that shall be performed by the developer. Requirements for developer actions are identified by appending the letter "D" to the element number.
b. Content and presentation of evidence elements: the evidence required, what the evidence shall demonstrate, and what information the evidence shall convey. Requirements for content and presentation of evidence are identified by appending the letter "C" to the element number.
c. Evaluator action elements: the activities that shall be performed by the evaluator. Requirements for evaluator actions are identified by appending the letter "E" to the element number.

6.1 Configuration Management (ACM)

6.1.1. Authorization Controls (ACM_CAP.3)

A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labeling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using.

Unique identification of the configuration items leads to a clearer understanding of the composition of the TOE, which in turn helps to determine those items which are subject to the evaluation requirements for the TOE.

Providing controls to ensure that unauthorized modifications are not made to the TOE, and ensuring proper functionality and use of the CM system, helps to maintain the integrity of the TOE.

Developer action elements:

6.1.1.1 ACM_CAP.3.1D. The developer shall provide a reference for the TOE.

6.1.1.2 ACM_CAP.3.2D. The developer shall use a Configuration Management (CM) system. The developer shall demonstrate that the identified CM system is employed for all TSF development.

6.1.1.3 ACM_CAP.3.3D. The developer shall provide CM documentation to the evaluation team that describes the CM system including the implementation and how the CM system has been used to control the development of the TSF.

Content and presentation of evidence elements:

6.1.1.4 ACM_CAP.3.1C. The reference for the TOE shall be unique to each version of the TOE.

6.1.1.5 ACM_CAP.3.2C. The TOE shall be labeled with its reference.

6.1.1.6 ACM_CAP.3.3C. The CM documentation shall include a configuration list and a CM plan.

6.1.1.7 ACM_CAP.3.4C. The configuration list shall describe the configuration items that comprise the TOE.

6.1.1.8 ACM_CAP.3.5C. The CM documentation shall describe the method used to uniquely identify the configuration items.

6.1.1.9 ACM_CAP.3.6C. The CM system shall uniquely identify all configuration items.

6.1.1.10 ACM_CAP.3.7C. The CM plan shall describe how the CM system is used.

6.1.1.11 ACM_CAP.3.8C. The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

6.1.1.12 ACM_CAP.3.9C. The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

6.1.1.13 ACM_CAP.3.10C. The CM system shall provide measures such that only authorized changes are made to the configuration items.

Evaluator action items:

6.1.1.14 ACM_CAP.3.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application Note: This component provides for three things. First, it requires that the TOE is identifiable by a customer, using things such as version and part numbers, to ensure that the proper thing has been installed. Second, it requires that the materials used to produce the TOE, such as source code and design documentation are identified. And third it requires that the production of the TOE be done in a controlled manner.

6.1.2. Coverage (ACM_SCP.1)

Developer action elements:

6.1.2.1 ACM_SCP.1.1D. The developer shall provide CM documentation.

Content and presentation of evidence elements:

6.1.2.2 ACM_SCP.1.1C. The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation.

6.1.2.3 ACM_SCP.1.2C. The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action items:

6.1.2.4 ACM_SCP.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2 Development (ADV)

6.2.1. Functional Specification (ADV_FSP.1)

The functional specification is a high-level description of the user-visible interface and behavior of the TSF. It is an instantiation of the TOE security functional requirements. The functional specification has to show that all the TOE security functional requirements are addressed.

Developer action elements:

6.2.1.1 ADV_FSP.1.1D. The developer shall provide a functional specification.

Content and presentation of evidence elements:

6.2.1.2 ADV_FSP.1.1C. The functional specification shall describe the TSF and its external interfaces using an informal style.

6.2.1.3 ADV_FSP.1.2C. The functional specification shall be internally consistent.

6.2.1.4 ADV_FSP.1.3C. The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

6.2.1.5 ADV_FSP.1.4C. The functional specification shall completely represent the TSF.

Evaluator action items:

6.2.1.6 ADV_FSP.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.1.7 ADV_FSP.1.2F. The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

Application Note: This component requires that the design documentation include a complete description of the TSF. In particular it needs to address the mechanisms which are used to meet the functional requirements of the PP. Other areas need to be addressed to the degree that they impact upon the functional requirements.

6.2.2. High-Level Design (ADV_HLD.2)

The high-level design of a TOE provides a description of the TSF in terms of major structural units (i.e. subsystems) and relates these units to the functions that they provide. The high-level design requirements are intended to provide assurance that the TOE provides an architecture appropriate to implement the TOE security functional requirements.

Developer action elements:

6.2.2.1 ADV_HLD.2.1D. The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

6.2.2.2 ADV_HLD.2.1C. The presentation of the high-level design shall be informal.

6.2.2.3 ADV_HLD.2.2C. The high-level design shall be internally consistent.

6.2.2.4 ADV_HLD.2.3C. The high-level design shall describe the structure of the TSF in terms of subsystems.

6.2.2.5 ADV_HLD.2.4C. The high-level design shall describe the security functionality provided by each subsystem of the TSF.

6.2.2.6 ADV_HLD.2.5C. The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

6.2.2.7 ADV_HLD.2.6C. The high-level design shall identify all interfaces to the subsystems of the TSF.

6.2.2.8 ADV_HLD.2.7C. The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

6.2.2.9 ADV_HLD.2.8C. The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

6.2.2.10 ADV_HLD.2.9C. The high-level design shall describe the separation of the TSF into TSP-enforcing and other subsystems.

Evaluator action items:

6.2.2.11 ADV_HLD.2.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.2.12 ADV_HLD.2.2E. The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

Application Note: This component requires that the design documentation include a breakdown of the TSF at a very coarse grain. Both the developer and evaluator need to carefully choose how a "subsystem" is defined for a particular TOE. There must be a balance between subsystems being so large that it is difficult to understand the functions, or being so small that it is difficult to understand how they fit into the system as a whole. Furthermore, it must be noted that the presentation need only be informal. This means that the interfaces between subsystems need to be

presented to general terms of how they interact, not to the level of presenting an API between them.

6.2.3. Correspondence Demonstration (ADV_RCR.1)

The correspondence between the various TSF representations (i.e. TOE summary specification, functional specification, high-level design, low-level design, implementation representation) addresses the correct and complete instantiation of the requirements to the least abstract TSF representation provided. This conclusion is achieved by step-wise refinement and the cumulative results of correspondence determinations between all adjacent abstractions of representation.

Developer action elements:

6.2.3.1 ADV_RCR.1.1D. The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

6.2.3.2 ADV_RCR.1.1C. For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action items:

6.2.3.3 ADV_RCR.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application Note: For this PP, this applies to ensure that the functional specification and high-level design are consistent with each other.

6.3 Life Cycle Support (ALC)

Development security is concerned with physical, procedural, personnel, and other security measures that may be used in the development environment to protect the TOE. It includes the physical security of the development location and any procedures used to select development staff.

6.3.1. Identification of Security Measures (ALC_DVS.1)

Developer action elements:

6.3.1.1 ALC_DVS.1.1D. The developer shall produce development security documentation.

Content and presentation of evidence elements:

6.3.1.2 ALC_DVS.1.1C. The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

6.3.1.3 ALC_DVS.1.2C. The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action items:

6.3.1.4 ALC_DVS.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.1.5 ALC_DVS.1.2E. The evaluator shall confirm that the security measures are being applied.

Application Note: For this PP, this is really an extension of configuration management system requirements to ensure that the TSF is not subverted by outsiders during development.

6.4 Security Testing (ATE)

This family addresses those aspects of testing that deal with completeness of test coverage. That is, it addresses the extent to which the TSF is tested, and whether or not the testing is sufficiently extensive to demonstrate that the TSF operates as specified.

6.4.1. Coverage (ATE_COV.2)

In this component, the objective is to establish that the TSF has been tested against its functional specification in a systematic manner. This is to be achieved through an examination of developer analysis of correspondence.

Developer action elements:

6.4.1.1 ATE_COV.2.1D. The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

6.4.1.2 ATE_COV.2.1C. The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

6.4.1.3 ATE_COV.2.2C. The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator action items:

6.4.1.4 ATE_COV.2.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.4.2. Depth (ATE_DPT.1)

The subsystems of a TSF provide a high-level description of the internal workings of the TSF. Testing at the level of the subsystems, in order to demonstrate the presence of any flaws, provides assurance that the TSF subsystems have been correctly realized.

Developer action elements:

6.4.2.1 ATE_DPT.1.1D. The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

6.4.2.2 ATE_DPT.1.1C. The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Evaluator action items:

6.4.2.3 ATE_DPT.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application Note: While the high-level design is to be used as the basis for testing, it is not required that internal interfaces between subsystems be tested.

6.4.3. Functional testing (ATE_FUN.1)

The objective is for the developer to demonstrate that all security functions perform as specified. The developer is required to perform testing and to provide test documentation.

Developer action elements:

6.4.3.1 ATE_FUN.1.1D. The developer shall test the TSF and document the results.

6.4.3.2 ATE_FUN.1.2D. The developer shall provide test documentation.

Content and presentation of evidence elements:

6.4.3.3 ATE_FUN.1.1C. The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

6.4.3.4 ATE_FUN.1.2C. The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

6.4.3.5 ATE_FUN.1.3C. The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

6.4.3.6 ATE_FUN.1.4C. The expected test results shall show the anticipated outputs from a successful execution of the tests.

6.4.3.7 ATE_FUN.1.5C. The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action items:

6.4.3.8 ATE_FUN.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.4.4. Independent Testing (ATE_IND.2)

The objective is to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests.

Developer action elements:

6.4.4.1 ATE_IND.2.1D. The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

6.4.4.2 ATE_IND.2.1C. The TOE shall be suitable for testing.

6.4.4.3 ATE_IND.2.2C. The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action items:

6.4.4.4 ATE_IND.2.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.4.4.5 ATE_IND.2.2E. The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

6.4.4.6 ATE_IND.2.3E. The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

Application Note: The choice of the subset tested and the sample tests executed is entirely at the discretion of the evaluator.

6.5 Vulnerability Assessment (AVA)

6.5.1. Examination of Guidance (AVA_MSU.1)

The objective is to ensure that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.

Developer action elements:

6.5.1.1 AVA_MSU.1.1D. The developer shall provide guidance documentation.

Content and presentation of evidence elements:

6.5.1.2 AVA_MSU.1.1C. The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

6.5.1.3 AVA_MSU.1.2C. The guidance documentation shall be complete, clear, consistent and reasonable.

6.5.1.4 AVA_MSU.1.3C. The guidance documentation shall list all assumptions about the intended environment.

6.5.1.5 AVA_MSU.1.4C. The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

Evaluator action items:

6.5.1.6 AVA_MSU.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.5.1.7 AVA_MSU.1.2E. The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

6.5.1.8 AVA_MSU.1.3. The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

Application Note: This requirement can be approached as testing by the evaluator to ensure that the guidance documents are correct. The content elements primarily reinforce the guidance requirements themselves.

6.5.2. Strength of TOE Security Function Evaluation (AVA_SOF.1)

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behavior can be made using the results of a quantitative or statistical analysis of the security behavior of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.

Developer action elements:

6.5.2.1 AVA_SOF.1.1D. The developer shall perform a strength of TOE security function analysis for each mechanism identified in the Security Target (ST) as having a strength of TOE security function claim.

Content and presentation of evidence elements:

6.5.2.2 AVA_SOF.1.1C. For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

6.5.2.3 AVA_SOF.1.2C. For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action items:

6.5.2.4 AVA_SOF.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.5.2.5 AVA_SOF.1.2E. The evaluator shall confirm that the strength claims are correct.

Application Note: For the TSPP, the requirement applies to the authentication mechanism as described in 5.2.3.

6.5.3. Developer Vulnerability Analysis (AVA_VLA.1)

A vulnerability analysis is performed by the developer to ascertain the presence of obvious security vulnerabilities, and to conform that they cannot be exploited in the intended environment for the TOE.

Developer action elements:

6.5.3.1 AVA_VLA.1.1D. The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

6.5.3.2 AVA_VLA.1.2D. The developer shall document the disposition of obvious vulnerabilities

Content and presentation of evidence elements:

6.5.3.3 AVA_VLA.1.1C. The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action items:

6.5.3.4 AVA_VLA.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.5.3.5 AVA_VLA.1.2E. The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

Application Note: The evaluator should consider the following with respect to the search for obvious flaws:

- Dependencies among functional components and potential inconsistencies in strength of function among interdependent functions;
- Potential inconsistencies between the TSP and the functional specification;
- Potential gaps or inconsistencies in the High Level Design, and potentially invalid assumptions about supporting hardware, firmware, and/or software required by the TSF;
- Potential gaps in the administrator guidance that enable the administrator to fail (a) to make effective use of TSF functions, (b) to understand or take actions that need to be performed, (c) to avoid unintended interactions among security functions, and (d) to install and/or configure the TOE correctly. In particular, failure to describe all the security parameters under the administrator's control and the effects of settings of (interacting combinations of) those parameters;
- Potential gaps in the user guidance that enable the user to fail to control functions and privileges as required to maintain a secure processing environment. Potential presence in the user guidance of information that facilitates exploitation of vulnerabilities;
- Open literature (e.g., CERT advisories, bug-traq mailing list) which may contain information on vulnerabilities on the TSF and these sources should be consulted.

6.6 Guidance Documents (AGD)

6.6.1. Administrator Guidance (AGD_ADM.1)

Administrator guidance refers to written material that is intended to be used by those persons responsible for configuring, maintaining, and administering the TOE in a correct manner for maximum security.

Developer action elements:

6.6.1.1 AGD_ADM.1.1D. The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

6.6.1.2 AGD_ADM.1.1C. The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

6.6.1.3 AGD_ADM.1.2C. The administrator guidance shall describe how to administer the TOE in a secure manner.

6.6.1.4 AGD_ADM.1.3C. The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

6.6.1.5 AGD_ADM.1.4C. The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

6.6.1.6 AGD_ADM.1.5C. The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

6.6.1.7 AGD_ADM.1.6C. The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

6.6.1.8 AGD_ADM.1.7C. The administrator guidance shall be consistent with all other documents supplied for evaluation.

6.6.1.9 AGD_ADM.1.8C. The administrator guidance shall describe all security requirements on the IT environment that are relevant to the administrator.

Evaluator action items:

6.6.1.10 AGD_ADM.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application Note: The content required by this component is quite comprehensive and broadly stated. In particular the contents need to address any of the mechanisms and functions provided to the administrator to meet the functional requirements of this PP. It should also contain warnings about certain actions that should not be done with the TOE. This could include turning on certain functions or installing certain software that would compromise the TSF.

6.6.2. User Guidance (AGD_USR.1)

User guidance refers to material that is intended to be used by non-administrative human users of the TOE, and by others (e.g. programmers) using the TOE's external interfaces.

Developer action elements:

6.6.2.1 AGD_USR.1.1D. The developer shall provide user guidance.

Content and presentation of evidence elements:

6.6.2.2 AGD_USR.1.1C. The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

6.6.2.3 AGD_USR.1.2C. The user guidance shall describe the use of user-accessible security functions provided by the TOE.

6.6.2.4 AGD_USR.1.3C. The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

6.6.2.5 AGD_USR.1.4C. The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

6.6.2.6 AGD_USR.1.5C. The user guidance shall be consistent with all other documentation supplied for evaluation.

6.6.2.7 AGD_USR.1.6C. The user guidance shall describe all security requirements on the IT environment that are relevant to the user.

Evaluator action items:

6.6.2.8 AGD_USR.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application Note: The content required by this component is quite comprehensive and broadly stated; in particular the contents needs to address any of the mechanisms and functions provided to users to meet the functional requirements of this PP. It should also contain warnings about certain actions (that could be done by users) which should not be done with the TOE.

6.7 Delivery and Operation (ADO)

The requirements for delivery call for system control and distribution facilities and procedures that provide assurance that the recipient receives the TOE that the sender intended to send, without any modifications.

6.7.1. Delivery Procedures (ADO_DEL.1)

Developer action elements:

6.7.1.1 ADO_DEL.1.1D. The developer shall document procedures for delivery of the TOE or parts of it to the user.

Developer action elements:

6.7.1.2 ADO_DEL.1.2D. The developer shall use the delivery procedures.

Content and presentation of evidence elements:

6.7.1.3 ADO_DEL.1.1C. The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action items:

6.7.1.4 ADO_DEL.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.7.2. Installation, generation, and start-up procedures (ADO_IGS.1)

Developer action elements:

6.7.2.1 ADO_IGS.1.1D. The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

6.7.2.2 ADO_IGS.1.1C. The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action items:

6.7.2.3 ADO_IGS.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.7.2.4 ADO_IGS.1.1E. The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

Application Note: The required documentation depends on the way in which a TOE is generated and installed. For example, the generation of a TOE from source code may be done at the development site, in which case the required documentation would be considered part of the design documentation. On the other hand, if some part of the TOE generation is done by the TOE administrator, it would be part of the administrative guidance. Similar circumstances could also apply to both installation and start-up procedures.

7. Rationale

7.1 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, security objective, and component that comprise the protection profile.

7.1.1. Complete Coverage – Threats, Organizational Security Policies, and Security Usage Assumptions

This section provides evidence demonstrating coverage of the threats, organizational security policies, and security usage assumptions by both IT and non-IT security objectives. Table 7.1.1.1 illustrates this coverage.

Table 7.1.1.1. Traceability of Security Objectives

Security Objectives	Threats	Organizational Security Policies	Security Usage Assumptions
IT Security Objectives			
O.KNOWN: The TSF shall ensure that, except for a well-defined set of allowed actions, all users are identified and authenticated before being granted access.	Insecure Security System	P.Access P.Confidential	A.Clearance A.Physical Authorization
O.ACCESS: The TSF shall allow access by authenticated users to those TOE resources for which they have been authorized, and deny access to those TOE resources for which they are not authorized.	Access Misuse; Insecure Security System; Fraud	P.Access P.Confidential	A.Clearance
O.AUTHORIZE: The TSF shall provide the ability to specify and manage "resource access permission" to be assigned to its users.	Access Misuse;	P.Administration P.Training P.TRA	A.TRA A.Clearance
O.BYPASS: The TSF shall prevent all software and users from bypassing or circumventing TOE security policy enforcement.	Access Misuse; Espionage; Insecure Security System	P.Access P.TRA	A.TRA A.Training A.Clearance
O.MISUSE: The TSF shall mitigate the threat of malicious actions by authenticated users	Fraud Access Misuse;	P.TMN P.Traceability P.Accountability P.Usage	A.Redress A.Audit A.Clearance
O.ACCOUNT: The TSF shall ensure that all TOE users can be held	Insecure Security System;	P.Accountability P.Usage	A.Redress A.Audit

Security Objectives	Threats	Organizational Security Policies	Security Usage Assumptions
accountable for their security-relevant actions.	Access Misuse; Espionage		
O.INFO-FLOW: The TSF shall ensure that any information flow control policies are enforced – (1) between TOE components and (2) at the TOE external interfaces.	Espionage; Access Misuse	P.Confidentiality P.TRA	A.InsecureRemote A.Insecure Network A.TRA
O.OBSERVE: The TSF shall ensure that its security status is not misrepresented to the administrator or user.	Insecure State Transition; Insecure Security System	P.Traceability	
O.DETECT: The TSF shall have the capability to detect system failure and breech of security.	Insecure Security System; Fraud	P.Traceability	A.Expertise
O.RECOVER: The TSF shall provide for recovery to a secure state following a system failure, discontinuity of service, or detection of a security flaw or breech.	Insecure State Transition;	P.Availability P.Resiliency	A.Expertise
O.AVAILABLE: The TSF shall protect itself from denial-of-service attacks, including shared resource exhaustion.	Denial of Service	P.Availability P.Resiliency	A.Environment A.NoBreakIns A.Hardware
O.NETWORK: Unless explicitly stand-alone, the TSF shall have the capability to meet the TOE security objectives in a distributed environment.	Physical Threat; Access Misuse	P.TMN	A.InsecureRemote A.Insecure Network A.Protocols A.Ingress
O.CONFIDENTIAL: The TOE shall have the ability to identify confidential information. Such information may be related to customers, system security, TRA or CALEA. The TOE shall release confidential information only to authorized users.	Access Misuse; Espionage;	P.Confidential P.Calea P.TMN P.TRA	A.Clearance A.TRA
Non-IT Security Objectives			

Security Objectives	Threats	Organizational Security Policies	Security Usage Assumptions
O.PHYSICAL: An administrator responsible for TOE security shall ensure that the TOE environment has adequate physical security to provide "reasonable safety" (as described earlier) to TOE resources.	Physical Threat	P.Administration P.Training	A.Environment
O.OPERATE: An administrator responsible for TOE security shall ensure that the TOE is delivered, installed, and operated in a manner which maintains IT security.	Insecure Security System	P.Administration	A.Expertise A.Training
O.MANAGE: An administrator responsible for TOE security shall ensure that the TOE is managed and administered in a manner that maintains IT security.	Insecure Security System	P.Administration	A.Audit A.Expertise
O.COMPLY: The TOE environment shall support full compliance with laws, regulations, and contractual agreements.	Access Misuse;	P.TMN P.Calea	A.Hardware

7.2 Security Requirements Rationale

This section provides evidence supporting the combined internal consistency and completeness of the functional and security requirements that comprise the TSPP.

Table 7.2-1 demonstrates that the functional components and assurance requirements selected for this profile provide complete coverage of the defined security objectives.

Table 7.2-1. Coverage of Security Objectives

Security Requirements	**SECURITY OBJECTIVES**
Functional Requirements	
5.1 Security Audit (FAU)	O.ACCOUNT
5.1 User Data Protection (FDP)	O.ACCESS O.BYPASS O.MISUSE O.RECOVER O.AVAILABLE O.EQUAL-ACCESS O.CALEA O.PHYSICAL O.DENIAL O.COMPLY
5.2 Identification and Authentication (FIA)	O.KNOWN O.ENTRY

	O.AUTHORIZE O.NETWORK
5.3 Security Management (FMT)	O.MANAGE O.OBSERVE O.DETECT O.RECOVER
5.4 Protection of the TOE Security Functions (FPT)	O.BYPASS O.INFO-FLOW
Assurance Requirements	
6.1 Configuration Management (ACM)	O.OPERATE O.MANAGE
6.2 Delivery and Operation (ADO)	O.OPERATE O.RESILIENCY
6.3 Development (ADV)	O.OPERATE
6.4 Guidance Documents (AGD)	O.MANAGE O.COMPLY
6.5 Life Cycle Support (ALC)	O.OPERATE O.MANAGE
6.6 Security Testing (ATE)	O.OPERATE
6.7 Vulnerability Assessment (AVA)	O.MANAGE

7.2.1 Internal Consistency of Requirements

This section describes the mutual support and internal consistency of the components selected for this profile. These properties are discussed for both functional and assurance components.

The functional components were selected from pre-defined CC components. The use of component refinement was accomplished in accordance with CC guidelines. An additional component was included to clarify the relationship of objects and security attributes.

Assignment, selection, and refinement operations were carried out among components using consistent computer security terminology. This helps to avoid the ambiguity associated with interpretations of meanings of terms between related components.

Multiple instantiation of identical or hierarchically related components was used to clearly state the required functionality that must exist in a TOE conformant with this profile.

8. Acronym List

CALEA - Communications Assistance for Law Enforcement Act.
CC - Common Criteria.
CCS - Common Channel Signaling network.
CMIP - Common Management Information Protocol.
DES - Digital Encryption Standard
DES3 - Triple DES
ESP - Encapsulated Security Payload
HMAC - Hash Message Authentication Code
IKE - Internet Key Exchange protocol
PP - Protection Profile.
SHA1 - Secure Hash Algorithm, version 1
SS7 - Signaling System-7 protocol.
ST - Security Target.
STP - Signal Transfer Point.
TMN - Telecommunications Management network.
TOE - Target of Evaluation.
TSF - TOE Security Function.
TSP - TOE Security Policy.
TSPP - Telecommunications Switch Protection Profile.